59516-042

REAL-TIME PACKET TRACEBACK AND ASSOCIATED PACKET MARKING STRATEGIES

Abstract of the Disclosure

To facilitate effective and efficient tracing of packet flows back to a trusted point as near as possible to the source of the flow in question, devices on the border of the trusted region are configured to mark packets with partial address information. Typically, the markings comprise fragments of IP addresses of the border devices in combination with fragment identifiers. By combining a small number of marked packets, victims or other interested parties are able to reconstruct the IP address of each border device that forwarded a particular packet flow into the trusted region, and thereby approximately locate the source(s) of traffic without requiring the assistance of outside network operators. Moreover, traceback can be done in real-time, e.g. while a DDoS attack is on-going, so that the attack can be stopped before the victim suffers serious damage.